Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application.

Claim 1 (currently amended): A method of communication between a first unit and a second unit via a telecommunications network, ~~in which~~ wherein the first unit comprises:

applications belonging respectively to a first family and a second family having a priori a lower degree of confidence than the first family; and

network access resources enabling the applications of the first and second family to communicate through the telecommunications network, the network access resources including a control layer,

the method comprising:

~~forcing~~ generating at least one request originating from an application of the second family~~, transmitted~~ for transmission over the network to the second unit~~,~~; and

processing said request in the control layer to force the request as transmitted over the network to include a mark associated with the second family of applications.

Claim 2 (canceled).

Claim 3 (currently amended): The method according to claim 1, wherein the processing of said request comprises ensuring that said mark~~, included in a request transmitted over the network and originating from an application of the second family, is forced to include~~ includes an indication of the nature and/or origin of ~~the~~ said application of the second family.

Claim 4 (previously presented): The method according to claim 3, wherein said application of the second family being signed, the mark included in the requests that originated therefrom is forced to include data relating to the certification of the signature.

Claim 5 (previously presented): The method according to claim 3, wherein the said application of the second family having been downloaded via the network from a download address, the mark included in the requests that originated therefrom is forced to include data relating to the download address of the application.

Claim 6 (currently amended): A method of communication between a first unit and a second unit via a telecommunications network, ~~in which~~ wherein the first unit comprises:

applications belonging respectively to a first family and to a second family having a priori a lower degree of confidence than the first family; and

network access resources enabling the applications of the first family and second family to communicate through the telecommunications network, the network access resources including a control layer,

the method comprising:

generating at least one first request originating from an application of the first family;

transmitting the first request over the network, the first request as transmitted including a mark associated with the first family;

generating ~~forcing~~ at least one second request originating from an application of the second family~~, transmitted~~ for transmission over the network to the second unit~~, to exclude~~; and

examining said second request in the control layer to force the second request as transmitted over the network not to include ~~a mark associated with the first family, the~~ said mark ~~being included in at least some of the requests transmitted over the network and originating from applications of the first family~~.

Claim 7 (currently amended): The method according to claim 6 wherein the second unit examines whether the mark is present in a request received over the network from the first unit, to assess a degree of confidence ~~to be attached to~~ for the said request.

Claim 8 (currently amended): The method according the claim 7, wherein, when the mark is present ~~the~~ in said request, the second unit also examines data included in ~~this~~ said mark, to assess a degree of confidence ~~to be attached to~~ for said request.

Claim 9 (previously presented): The method according to claim 8, wherein said data examined by the second unit comprises data relating to the certification of a signature of the application from which the request originated.

Claim 10 (previously presented): The method according to claim 8, wherein said data examined by the second unit comprise data relating to a download address of the application from which the request originated.

Claim 11 (previously presented): The method according to claim 6, wherein the requests comprise HTTP requests, and the mark is inserted in the headers of the HTTP requests.

Claim 12 (currently amended): The method according to ~~any one of the preceding~~ claim 1 ~~6~~, wherein the network access resources comprise a virtual machine and the control layer comprises ~~in which the requirement relating to the mark is controlled by a~~ software ~~layer~~ belonging to ~~a~~ said virtual machine ~~with which the first unit is provided~~, the applications of the second family being able to access the network only via the virtual machine and ~~the~~ said software ~~layer~~.

Claim 13 (previously presented): The method according to claim 12, wherein the virtual machine is a Java virtual machine.

Claim 14 (currently amended): A communication terminal, comprising:

~~means for communicating with a second unit via telecommunications network, the communication terminal further comprising~~ applications belonging respectively to a first family and a second family having a priori a lower degree of confidence than the first family; and

network access resources enabling the applications of the first and second family to communicate through a telecommunications network with at least one remote unit, the network access resources including a control layer,

wherein the control layer is ~~means for communicating are~~ adapted to examine a ~~force~~

~~at least one~~ request originating from an application of the second family for transmission over the network to the remote unit so that the request as~~,~~ transmitted over the network ~~to the second unit, to include~~ includes a mark associated with the second family of applications.

Claim 15 (currently amended): A communication terminal, comprising:

~~means for communicating with a second unit via a telecommunications network, the communication terminal further comprising~~ applications belonging respectively to a first family and a second family having a priori a lower degree of confidence than the first family; and

network access resources enabling the applications of the first and second family to communicate through a telecommunications network with at least one remote unit, the network access resources including a control layer,

wherein the control layer is ~~means for communicating are~~ adapted to examine a ~~force at least one~~ request originating from an application of the second family for transmission over the network to the remote unit so that the request as~~,~~ transmitted over the network ~~to the second unit, to exclude~~ does not include a mark associated with the first family, ~~the~~ said mark being included in at least some ~~of the~~ requests transmitted over the network and originating from applications of the first family.

Claim 16 (previously presented): The method according to claim 1, wherein each request originating from an application of the second family, transmitted over the network to the second unit, is forced to include a mark associated with the second family of applications.

Claim 17 (previously presented): The method according to claim 6, wherein each request originating from an application of the second family, transmitted over the network to the second unit, is forced to exclude a mark associated with the first family.

Claim 18 (new): The method according to claim 6, wherein the network access resources comprise a virtual machine and the control layer comprises software belonging to said virtual machine, the applications of the second family being able to access the network only via the virtual machine and said software.

Claim 19 (new): The method according to claim 18, wherein the virtual machine is a Java virtual machine.